The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
06/29/2016

SUBJECT:
Multiple Vulnerabilities in Symantec Products Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered for the Symantec Decomposer Engine, which is used in various configurations by multiple Symantec products. The most severe of these vulnerabilities could allow for remote code execution. Successfully exploiting these vulnerabilities could allow an attacker to run remote code on the affected system. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in a denial-of-service condition.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild. However, proof-of-concept code was released by Google's Project Zero.

SYSTEMS AFFECTED:
- Advanced Threat Protection
- Symantec Data Center Server versions 6.6 MP1, 6.5 MP1
- Symantec Critical System Protection versions 5.2.9 MP6
- Symantec Embedded Systems Critical System Protection versions 1.0 MP5, 6.5.0 MP1
- Symantec Web Security .Cloud
- Email Security Server .Cloud
- Symantec Web Gateway
- Symantec Endpoint Protection prior to version 12.1 RU6 MP5
- Symantec Endpoint Protection for Mac version 12.1.6 RU6 MP4 and prior
- Symantec Endpoint Protection for Linux prior to version 12.1 RU6 MP5
- Symantec Protection Engine prior to versions 7.05 HF01, 7.5.3 HF03, 7.5.4 HF01, 7.8.0 HF01
- Symantec Protection for SharePoint Servers prior to versions SPSS_6.0.3_To_6.0.5_HF_1.5, SPSS_6.0.6_HF_1.6
- Symantec Mail Security for Microsoft Exchange prior to versions SMSMSE_7.0_3966002_HF1.1, SMSMSE_7.5_3966008_VHF1.2
- Symantec Mail Security for Domino prior to versions SMSDOM_8.0.9_HF1.1, SMSDOM_8.1.3_HF1.2
- CSAPI prior to version 10.0.4 HF01
- Symantec Message Gateway prior to version 10.6.1-4
- Symantec Message Gateway for Service Providers prior to versions SMG-SP 10.6 patch 253, SMG-SP 10.5 patch 254
- Norton Product Family prior to NGC 22.7
    - Norton Antivirus
    - Norton Security

    - Norton Security with Backup
    - Norton Internet Security
    - Norton 360
- Norton Security for Mac prior to version 13.0.2
- Norton Power Eraser prior to version 5.1
- Norton Bootable Removal Tool prior to version 2016.1

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: **Low**

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in the Symantec Antivirus Decomposer Engine, the most severe of which could allow for remote code execution. An attacker can exploit this issue by sending a specially crafted file to execute remote code. When the maliciously-formatted file is parsed by the engine, it may cause memory corruption, integer overflow or buffer overflow. The details of these vulnerabilities are as follows:

- RAR decompression memory access violation (CVE-2016-2207).
- Dec2SS buffer overflow (CVE-2016-2209).
- Dec2LHA buffer overflow (CVE-2016-2210).
- CAB decompression memory corruption (CVE-2016-2211).
- MIME message modification memory corruption (CVE-2016-3644).
- TNEF integer overflow (CVE-2016-3645).
- ZIP decompression memory access violation (CVE-2016-3646).

Successful exploitation of these vulnerabilities could allow for remote code execution on the affected system. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in a denial-of-service condition.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Symantec immediately after appropriate testing.
- Ensure all productdefinitions are up-to-date to mitigates some of the aforementioned vulnerabilities.
- Verify no unauthorized system modifications have occurred on system before applying the patch.

- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the principle of Least Privilege to all systems and services.

REFERENCES:

Symantec:
https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160628_00

Google Project Zero:
http://googleprojectzero.blogspot.com/2016/06/how-to-compromise-enterprise-endpoint.html
https://bugs.chromium.org/p/project-zero/issues/detail?id=820

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2207
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2209
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2210
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2211
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3644
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3645
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3646